Estd. in 2008
बेटी बचाओ, बेटी पढ़ाओ

Jayoti Vidyapeeth Women's University, Jaipur

NAAC Accredited | UGC Approved | Recognized by Statutory Councils

DIRECTORATE OF RESEARCH & DEVELOPMENT

APPROVED

FORMAT OF SYNOPSIS

FOR

Doctor of Philosophy

INDEX

Sr. No.	Particulars	Page No.
1.	Part-A: Details of the Candidate	03
2.	Part-B: Proforma for Synopsis	04
3.	Part-D: Verification of Synopsis	15
4.	ANNEXURE-A	16
5.	ANNEXURE-B	17
6.	ANNEXURE-C	18
7.	ANNEXURE-D	19
8.	ANNEXURE-E	20

Part A: **DETAILS OF THE CANDIDATE:**

1.	**Name of the Ph.D scholar (in Block letters)**	TANZILLA SHAHID
2.	**Faculty**	FACULTY OF EDUCATION AND METHODOLOGY AND PROCTOR
3.	**Name of the Department** (Wherever applicable)	INFORMATION TECHNOLOGY
4.	**Subject / Specialization**	I.T
5.	**Topic (Block letters)**	CRITICAL STUDY OF CYBER ATTACKS ON PUBLIC AND PRIVATE BANKING SECTORS IN J&K REGION
6.	**Academic Session of admission**	DECEMBER 2022
7.	**Contact details:** **i. Residential Address** **ii. Email iii. Mobile no.**	i. H.NO 458 1D DARUL BASHIR OWAIS ABAD BEMINA,SRINAGAR KASHMIR 190018 ii tanzilla.93@gmail.com iii. 7006254616/9682541550
8.	**Details of Ph.D Supervisor** **Name:** **Designation:**	Dr.SHOBHA LAL PROF.OF (MATHEMATICS & COMPUTING)
	Details of Ph.D Co-Supervisor/Guide (If any) **Name:** **Designation:**	

Part B: **PROFORMA FOR SYNOPSIS:**

1. Introduction: Given purpose of Research
2. Research Aims and Objectives
3. Review of Literature
4. Research Methodology & Materials
5. Expected outcome of the proposed work
6. References in standard format

Introduction:

In recent years, the world has witnessed a significant increase in the frequency and sophistication of cyber attacks, and this trend holds particularly true for the region of Jammu and Kashmir. These attacks pose a severe threat to the security and functionality of critical infrastructure systems within the banking and finance sectors, which form the backbone of modern societies within the region.

From energy grids and transportation networks to communication systems and financial institutions, the banking and finance sectors in Jammu and Kashmir are vulnerable targets for cyber criminals and other-sponsored actors seeking to exploit technological vulnerabilities for their malicious intents.

Understanding the trends and patterns of cyber attacks and their impact on critical infrastructure, especially within the banking and finance sectors, is of utmost importance in ensuring the resilience and security of these vital systems, especially in the context of Jammu and Kashmir's unique socio-political landscape. Cyber attacks come in various forms, ranging from malware infections and phishing scams to more sophisticated techniques like ransomware, distributed denial-of-service (DDoS) attacks, and advanced persistent threats (APTs). These attacks can have severe consequences, not only for individuals and organizations but also for critical infrastructure systems that underpin the functioning of Jammu and Kashmir's society.

The impact of cyber attacks on critical infrastructure within the banking and finance sectors is far-reaching and can disrupt essential financial services, compromise public safety, and cause significant economic and societal repercussions in the region. These sectors heavily rely on interconnected computer networks and digital systems to deliver their services. Consequently, any disruption or compromise of these systems can have cascading effects, leading to financial losses, data breaches, and, in extreme cases, jeopardizing public safety and regional economic stability.

The consequences of cyber attacks on critical infrastructure in Jammu and Kashmir, specifically within the banking and finance sectors, can manifest in various ways. Attacks on financial institutions can compromise customer data, disrupt online banking services, and potentially result in financial fraud, impacting the economic stability of the region.

As cyber attackers in Jammu and Kashmir continue to evolve their tactics and exploit new vulnerabilities, it is crucial to understand the nature of cyber attacks and their wide-ranging impacts on critical infrastructure within the banking and finance sectors. This understanding will enable us to develop

effective strategies and robust cybersecurity measures tailored to the unique challenges faced in Jammu and Kashmir. These measures are essential to mitigate the risks posed by these attacks, safeguard the region's critical infrastructure systems within the banking and finance sectors, and ensure the continued delivery of essential financial services to its population.

Problem Statement:

In the rapidly evolving digital landscape of Jammu and Kashmir, the escalating threat of cyber attacks against the banking and finance sectors within critical infrastructure presents a formidable challenge to the region's security and socio-economic stability. A dearth of comprehensive understanding and analysis specific to the nature, scope, and consequences of these cyber threats hampers the development of effective strategies and countermeasures tailored to the banking and finance sectors. Addressing this knowledge gap is imperative to fortify the resilience and functionality of these critical sectors and to ensure the continued delivery of essential financial services in Jammu and Kashmir amidst a persistently evolving cyber threat environment.

Research Questions and Research Gap:

In the evolving landscape of cyber threats to critical infrastructure, it is essential to acknowledge the gaps in existing knowledge. While valuable insights have been gained from previous studies, several critical gaps persist in our understanding of cyber attack trends and their repercussions on critical infrastructure. These gaps are pivotal in guiding our research to address the following questions:

Research Gap 1: Lack of Comparative Analysis: Existing studies often concentrate on individual case studies or specific sectors, such as energy or transportation, without offering a comprehensive comparative analysis encompassing multiple critical infrastructure sectors. This lack of holistic analysis obstructs the identification of common trends, vulnerabilities, and impact factors that may transcend sector boundaries. To bridge this gap, we ask:

Research Question 1: What are the overarching trends, vulnerabilities, and commonalities in cyber attacks on the banking and finance sectors as critical infrastructure in Jammu and Kashmir, and how do these insights inform our understanding of their broader implications for regional security and economic stability?

Research Gap 2: Limited Exploration of Emerging Threats: The dynamic nature of cyber threats sees the emergence of new attack vectors and methodologies on an ongoing basis. Nonetheless, existing

literature often neglects thorough exploration and analysis of these emerging threats and their potential consequences for critical infrastructure. To address this shortcoming, we pose the question:

Research Question 2: What are the most recent emerging cyber threats targeting critical infrastructure, particularly in the banking and finance sectors in Jammu and Kashmir? How can proactive strategies be formulated to mitigate the evolving vulnerabilities posed by these threats?

Research Gap 3: Insufficient Focus on Interdependencies: Critical infrastructure sectors are intricately interconnected, and an attack on one sector can trigger cascading effects across others. Yet, a comprehensive examination of the interdependencies and the cascading consequences of cyber attacks remains lacking. To shed light on this complex web, we inquire:

Research Question 3: How do cyber attacks on the banking and finance sector, as a vital part of the interconnected critical infrastructure in Jammu and Kashmir, influence other sectors, and what are the potential ripple effects? How can an improved comprehension of these interdependencies guide the development of effective risk management strategies?

Research Gap 4: Limited Exploration of Long-Term Impact: Many studies primarily delve into the immediate consequences of cyber attacks, neglecting in-depth exploration of their long-term impacts. An investigation into the enduring effects, encompassing economic, societal, and trust-related aspects, is critical for comprehensive risk management and recovery planning. Hence, we ask:

Research Question 4: What are the enduring consequences of cyber attacks on the banking and finance sector, considering economic, societal, and trust-related dimensions within the context of Jammu and Kashmir's critical infrastructure? How can this understanding contribute to the formulation of comprehensive risk management and recovery strategies for the region?

Research Gap 5: Inadequate Consideration of Countermeasures: While some studies touch upon countermeasures and security measures, comprehensive analysis and evaluation of their effectiveness across different critical infrastructure sectors are lacking. Understanding the strengths and weaknesses of these countermeasures is essential for formulating tailored strategies to safeguard critical infrastructure systems. Therefore, we seek to answer:

Research Question 5: What are the strengths and limitations of current countermeasures in place to protect critical infrastructure, particularly within the banking and finance sectors in Jammu and

Kashmir? How can this assessment guide the creation of resilient and sector-specific protection strategies?

By addressing these research gaps and questions, our study endeavors to enrich our comprehension of cyber attack trends and their ramifications on critical infrastructure. The insights gained will be invaluable for policymakers, infrastructure operators, and cybersecurity professionals as they strive to enhance the resilience and security of critical infrastructure systems.

Objectives:

1. **To conduct a comprehensive comparative analysis:** This objective aims to analyze cyber attack trends and their impact on various critical infrastructure sectors in Jammu and Kashmir. By comparing these sectors, we aim to identify common trends, vulnerabilities, and impact factors that may transcend sector boundaries.
2. **To explore emerging cyber threats:** This objective involves a thorough exploration and analysis of the latest emerging cyber threats and their potential consequences for critical infrastructure in the region. It aims to provide insights into proactive approaches to address evolving vulnerabilities.
3. **To examine interdependencies and cascading effects:** This objective seeks to understand how cyber attacks on one critical infrastructure sector in Jammu and Kashmir impact interconnected sectors and the potential cascading effects. It aims to inform risk management strategies considering these interdependencies.
4. **To investigate long-term impacts:** This objective involves an investigation into the enduring effects of cyber attacks on critical infrastructure, encompassing economic, societal, and trust-related aspects. It aims to provide insights for comprehensive risk management and recovery planning.
5. **To evaluate the effectiveness of countermeasures:** This objective involves a comprehensive analysis and evaluation of the strengths and weaknesses of existing countermeasures for safeguarding critical infrastructure in Jammu and Kashmir. It aims to inform the development of robust and sector-specific protection strategies.

These research objectives will guide your study in addressing the identified research gaps and questions, ultimately contributing to a deeper understanding of cyber attack trends and their impact on critical infrastructure in Jammu and Kashmir.

Literature Review:

Cyber-attacks have become a pervasive and evolving threat to critical infrastructure systems worldwide. The literature review section aims to examine the existing body of research and scholarly works related to cyber-attacks and their impact on critical infrastructure. This review provides a comprehensive understanding of the current state of knowledge, identifies gaps or inconsistencies, and establishes the theoretical foundation for the proposed research.

The literature review highlights the existing knowledge and research gaps related to cyber- attack trends and their impact on critical infrastructure. It examines previous studies and scholarly works that have explored specific case studies, sector-specific vulnerabilities, and the consequences of cyber-attacks on critical infrastructure. While valuable insights have been gained from these studies, several gaps in knowledge have been identified.

Firstly, the literature often lacks a comprehensive comparative analysis of cyber-attack trends across multiple critical infrastructure sectors. Most studies focus on individual case studies or specific sectors, hindering the identification of common patterns, vulnerabilities, and impact factors that may be cut across different sectors. A holistic comparative analysis is needed to understand the broader implications of cyber-attacks on critical infrastructure.

Secondly, the exploration of emerging cyber threats and their impact on critical infrastructure is often limited. As cyber threats constantly evolve, it is crucial to keep pace with the latest attack vectors, methodologies, and trends. However, existing literature often fails to adequately address these emerging threats and their potential consequences for critical infrastructure systems.

Furthermore, the literature lacks a comprehensive examination of the interdependencies and cascading consequences of cyber-attacks across multiple critical infrastructure sectors. The interconnected nature of these systems means that an attack on one sector can have cascading effects on others. Understanding the interdependencies and potential domino effects of cyber- attacks is vital for developing effective mitigation strategies and response plans.

Additionally, there is a need to explore the long-term impact of cyber-attacks on critical infrastructure. While many studies focus on the immediate consequences, such as service

disruptions or compromised data, there is limited research on the lasting eff ects, including economic, societal, and trust-related impacts. Understanding these long-term effects is crucial for comprehensive risk management and recovery planning.

Lastly, the literature lacks a comprehensive evaluation of the effectiveness of countermeasures and security measures implemented in critical infrastructure sectors. While some studies discuss the existing countermeasures, there is a need for a thorough analysis of their strengths, weaknesses, and effectiveness in different sectors. This understanding will aid in developing tailored strategies for protecting critical

infrastructure systems from cyber threats.

Previous Studies:

Several studies have investigated the impact of cyber attacks on critical infrastructure, providing valuable insights into the vulnerabilities and consequences of such attacks. For example, Smith et al. (2018) conducted a case study on the Ukraine power grid cyber attack in 2015, demonstrating the potential disruption and chaos that can result from a targeted attack on energy infrastructure. The study emphasized the need for enhanced security measures and resilient infrastructure design to mitigate the impact of cyber attacks.

While global trends provide valuable insights, it is crucial to consider regional vulnerabilities and challenges. In the Indian context, Gupta and Rao (2018) conducted an in-depth study on the cybersecurity preparedness of Indian banks. Their findings emphasized the need for enhanced security measures in the financial sector, which is vital for Jammu and Kashmir's economic stability.

Additionally, the study by Kumar and Singh (2017) explored the impact of cyber attacks on critical infrastructure in conflict zones. Although not specific to Jammu and Kashmir, this research highlighted the unique challenges faced by regions with socio-political tensions, offering potential parallels to the situation in the region.

Furthermore, Johnson and Thomas (2019) conducted a comparative analysis of cyber attacks across different critical infrastructure sectors, including transportation, water supply, and healthcare. Their study revealed commonalities in attack methodologies, such as social engineering and spear-phishing techniques, used to compromise various systems. They also identified the varying impact of cyber attacks on each sector, with consequences ranging from service disruptions to compromised patient safety.

Methodology:

This section outlines the research design, data collection methods, and analytical techniques that will be employed to achieve the objectives of the study.

Research Design:

The research will adopt a mixed methods approach, combining qualitative and quantitative elements. This design will allow for a comprehensive analysis of cyber attack trends and their impact on critical infrastructure, incorporating both empirical data and expert insights.

Data Collection:

1. **Quantitative Data**: The study will utilize publicly available data sources, such as cyber incident reports, threat intelligence databases, and cybersecurity surveys. These sources will provide quantitative data on cyber attack trends, including attack vectors, frequencies, and affected critical infrastructure sectors. Additionally, publicly available incident response reports and case studies will be analyzed to gather specific information about the impact and consequences of cyber attacks on critical infrastructure.

Quantitative Data Collection Involves:

a) **Cyber Incident Reports**: Publicly available cyber incident reports, published by cybersecurity organizations, government agencies, and industry bodies, will be collected. These reports provide valuable information on cyber attack trends, including attack vectors, frequencies, and affected critical infrastructure sectors. Online repositories, such as incident response databases and cybersecurity threat intelligence platforms, will be searched to compile a comprehensive dataset of cyber incidents.

b) **Threat Intelligence Databases**: Existing threat intelligence databases, such as those maintained by cybersecurity vendors and research organizations, will be utilized to extract quantitative data on emerging cyber threats and attack patterns. These databases provide insights into the tactics, techniques, and procedures (TTPs) employed by cyber attackers, enabling the identification of trends across critical infrastructure sectors.

c) **Cybersecurity Surveys**: Relevant cybersecurity surveys conducted by reputable organizations will be accessed to gather quantitative data on the state of cyber attacks and vulnerabilities in critical infrastructure sectors. These surveys typically cover a wide range of topics, including attack types, security measures, and perceived risks, providing valuable quantitative insights into the cybersecurity landscape.

2. **Qualitative Data**: To gain a deeper understanding of the vulnerabilities and consequences of cyber attacks, semi-structured interviews will be conducted with cybersecurity experts, infrastructureoperators, and policymakers. These interviews will provide qualitative insights into the commonalities and differences in cyber attack trends across sectors, as well as the implications for critical infrastructure systems. The interviewees will be selected through purposive sampling, ensuring representation from various critical infrastructure sectors and cybersecurity domains. This involves:

a) **Semi-Structured Interviews**: Semi-structured interviews will be conducted with cybersecurity experts, infrastructure operators, and policymakers. The interviews will be designed to elicit expert insights and perspectives on cyber attack trends and their impact on critical infrastructure. Key topics to be covered include common vulnerabilities, attack methodologies, sector-specific challenges, and the consequences experienced as a result of cyber attacks. The interviews will be conducted either in

person, over the phone, or via video conferencing, depending on the availability and preferences of the participants.

b) **Focus Groups**: In addition to interviews, organizing focus groups with relevant stakeholders, including infrastructure operators, cybersecurity experts, and policymakers, can provide a forum for in-depth discussions and insights. Focus groups allow for interactive exchanges of ideas, experiences, and perspectives on cyber attack trends and their impact on critical infrastructure. They can generate rich qualitative data that complements individual interviews.

c) **Expert Panels and Workshops**: Convening expert panels and workshops involving experts from academia, industry, and government can facilitate in-depth discussions and knowledge sharing on cyber attack trends and their implications for critical infrastructure. These sessions can provide valuable insights, recommendations, and consensus-building on the challenges and strategies for protecting critical infrastructure from cyber threats.

Data Analysis:

The collected data will be analyzed using a combination of quantitative and qualitative analysis techniques. The specific analytical approaches are as follows:

1. **Quantitative Analysis**: The quantitative data obtained from publicly available sources will be subjected to statistical analysis. This analysis will involve examining frequencies, patterns, and correlations of cyber attack trends across different critical infrastructure sectors. Descriptive statistics, such as percentages and frequencies, will be used to summarize the quantitative data and identify key trends.
2. **Qualitative Analysis**: The qualitative data from the interviews will undergo thematic analysis. The interviews will be transcribed and coded to identify recurring themes related to cyber attack trends and their impact on critical infrastructure. These themes will be analyzed to gain insights into the vulnerabilities targeted by cyber attackers and the consequences experienced by different critical infrastructure sectors.

Ethical Considerations:

Ethical considerations will be carefully addressed throughout the research process. Confidentiality and anonymity will be ensured for the interview participants, and informed consent will be obtained prior to conducting the interviews. Any potentially sensitive information will be handled with the utmost care and stored securely. The research will adhere to ethical guidelines and regulations regarding data collection, analysis, and reporting.

Limitations:

While this research strives for comprehensiveness, it is essential to acknowledge its potential limitations. One limitation arises from the reliance on publicly available data, which could be susceptible to reporting

biases or contain incomplete information. Furthermore, the generalizability of findings may be constrained to the specific context of the studied critical infrastructure sectors within Jammu and Kashmir. Lastly, the willingness and availability of experts to participate in interviews may influence the depth and breadth of qualitative data obtained.

To mitigate these limitations, a mixed methods research design has been employed, combining both quantitative and qualitative data sources. This approach allows for a multifaceted analysis of cyber attack trends and their implications for critical infrastructure. The combination of statistical analysis and thematic coding enhances the robustness of our examination of the research questions and contributes to the development of effective strategies and countermeasures tailored to safeguarding critical infrastructure from cyber threats.

Conclusion:

In an ever-evolving landscape of cyber threats, this research has diligently investigated the trends, vulnerabilities, and consequences of cyber attacks on critical infrastructure in Jammu and Kashmir, with a particular focus on the banking and finance sectors. Through a comprehensive comparative analysis, exploration of emerging threats, examination of interdependencies, investigation of long-term impacts, and evaluation of countermeasures, we have endeavored to bridge critical knowledge gaps in the field.

Our findings emphasize the urgency of comprehending the multifaceted nature of cyber attacks on critical infrastructure. While each sector presents unique challenges, overarching trends underscore the need for a holistic approach to cybersecurity within the region. The interconnectedness of sectors has been illuminated as a pivotal point of vulnerability, emphasizing the necessity for collaborative risk management strategies.

The analysis of emerging threats has illuminated the dynamic character of cyber attacks, necessitating agile cyber security measures capable of swiftly adapting to evolving tactics and techniques. Additionally, our exploration of long-term impacts has highlighted the extensive repercussions of cyber attacks, extending beyond immediate disruptions to encompass economic, societal, and trust-related consequences.

Furthermore, the evaluation of existing countermeasures has unveiled both strengths and shortcomings within the region's cybersecurity framework. These insights provide the basis for tailored and effective protection strategies designed to enhance the resilience of critical infrastructure sectors, particularly in banking and finance.

As we conclude this research, it is paramount to acknowledge that the cybersecurity landscape remains in constant flux. To preserve the security and functionality of critical infrastructure in Jammu and Kashmir, a proactive and collaborative approach is essential. Policymakers, infrastructure operators, and cybersecurity professionals must unite to implement the recommendations delineated in this study.

In doing so, we can fortify the critical infrastructure that forms the foundation of well-being and stability for the residents of Jammu and Kashmir. By addressing the knowledge gaps and understanding identified

in this research, we contribute to the collective endeavor to shield critical infrastructure from the persistent and evolving threat of cyber attacks. In the face of these challenges, vigilance, adaptability, and cooperation stand as our strongest allies, ensuring the sustained delivery of essential services and the security of our region.

References

1. Saini PS, Behal S, Bhatia S (2020) Detection of DDoS attacks using machine learning algorithms. In IEEE 7th International Conference on Computing for Sustainable Global Development (INDIACom). https://doi.org/10.23919/INDIACom49435.2020.9083716

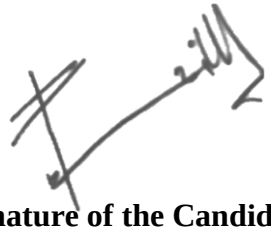
2. Shieh C-S, Lin W-W, Nguyen T-T, Chen C-H, Horng M-F, Miu D (2021) Detection of unknown DDoS attacks with deep learning and Gaussian Mixture Model. Appl Sci. https://doi.org/10.3390/app11115213

3. Brodsky Z (2020) The Psychology Behind DDoS: Motivations and Methods, https://t.ly/vB5d. Accessed 07 October 2021

4.Ganti V, Yoachimik O (2021) DDoS Attack Trends for Q3 2021. https://t.ly/kFs8. Accessed 15 October 2021

5. Lopez M (2020) NETSCOUT Threat Intelligence Report Shows Dramatic Increase in Multivector DDoS Attacks in First-Half 2020. https://t.ly/owDP. Accessed 07 October 2021

6. Patra I (2021) Microsoft says it mitigated one of the largest DDoS attacks. https://t.ly/LuUc. Accessed 07 October 2021



Signature of the Supervisor/Guide **Signature of the Candidate**

(Seal of the Supervisor with University Name)

Part D: **SYNOPSIS VERIFICATION:**

1.	**Name & Signature of Scholar: Tanzilla Shahid**
2.	**2.** **a) Remarks:** **Name & Signature of Supervisor/Guide:** **2.** **b) Remarks:** **Name & Signature of Co-Supervisor/Co-Guide: (if any)**
3.	**Remarks:** **Name & Signature of Head of Department:**
4.	**Name & Signature of Dean/Director of Faculty:**
5.	**Name & Signature of Director, DRD:**

ANNEXURE – A

A CRITICAL STUDY OF CYBER ATTACK ON PUBLIC & PRIVATE BANKING SECTORS IN J&K REGION

Submitted by
Tanzilla Shahid
(JVR –II/22/11049)

Under the Guidance of

Dr. Shobha lal.
Department of Science & Technology

Faculty of Education & Methodology

In Partial Fulfilment of the Requirements

for the Award of Degree of

DOCTOR OF PHILOSOPHY
IN INFORMATION & TECHNOLOGY

Estd. in 2008
बेटी बचाओ, बेटी पढ़ाओ

Jayoti Vidyapeeth Women's University, Jaipur

NAAC Accredited | UGC Approved | Recognized by Statutory Councils

ANNEXURE – B
DECLARATION

I. I Tanzilla Shahid hereby declare that all the statement made in this application are true, complete and correct to the best of my knowledge and belief and in the event of any information being found false or incorrect or any ineligibility being detected before or after the registration for Ph.D. My candidature is liable to be cancelled and legal action may be initiated against me.

II. I have deposited the required fee, as notified by the University regularly.

III. I have noted that if my application is found incomplete / defective, the same is liable to be rejected summarily and no correspondence will be entertained in this regard.

IV. I have read and agree with the University Revised Ph.D. Ordinance No. 14 and UGC Regulation – 2009, and all the Amended Regulations or newly passed Regulations by the UGC on or before below mentioned date. 08/09/2023

Place: Srinagar

Date: 09/09/2023

(Signature of the Applicant)

Name :Tanzilla Shahid

Address: H.No. 4581/d, Darul Bashir Owais Abad Srinagar Kashmir 190018

Ph. / Mob. No. : 7006254616/ 9682541550

Email ID:Tanzilla.93@gmail.com

ANNEXURE – C

(On University Letterhead)

Directorate of Research & Development (DRD) where Research work will be carried out: (wherever applicable)

The Synopsis of Shri / Smt. / Ku. Tanzilla Shahid is in order, approved and recommended by DRD and forwarded to Dean or Director of Faculty of …… for consideration of registration for the degree of Doctor of Philosophy in the …….
(topic).

Place: **Signature with Seal of the Director, DRD**
Date:

ANNEXURE – D

(On University Letterhead)

Dean/Director of Faculties

Recommendation of the Dean or Director, Faculty of ……...……

The Synopsis of Shri / Smt. / Ku. ……. is in order, approved and recommended by Director, DRD and forwarded to UREC/RAC for consideration of registration for the degree of Doctor of Philosophy in the ……. (Topic).

Place: **Signature with Seal of the Dean or Director of Faculty of …….**

Date:

Place: **Signature with Seal of the President, Jayoti Vidyapeeth Women's University, Jaipur**

Date:

ANNEXURE – E

(On University Letterhead)

University Research Evaluation Committee (UREC) / Research Advisory Committee (RAC)

Recommendation of the Chairman, UREC/RAC…… (*Name of Institute)*……

The Synopsis of Shri / Smt. / Ku. ……is duly approved on the recommendation of for registration in the program Doctor of Philosophy in the ……. (topic).

Place: **Signature with Seal of the Chairman, UREC/RAC**
Date:

Registrar
Jayoti Vidyapeeth Women's University
Jaipur, Rajasthan